UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AIRBNB, INC., *Plaintiff,* v. CITY OF NEW YORK, *Defendant.*	CIVIL ACTION NOS. 18-cv-7712-PAE 18-cv-7742-PAE Hon. Paul A. Engelmayer
HOMEAWAY.COM, INC., *Plaintiff,* v. CITY OF NEW YORK, *Defendant.*	

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS' MOTIONS FOR PRELIMINARY INJUNCTION

Mitchell L. Stoltz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: mitch@eff.org

Dated: October 1, 2018

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES ii

INTEREST OF AMICUS CURIAE 1

INTRODUCTION 3

ARGUMENT 4

I. The Short-Term Residential Rentals Ordinance Will Sweep in Sensitive and Revealing Data on Tens of Thousands of Innocent Individuals. 4

II. The Ordinance Violates the Fourth Amendment. 7

A. Users Have a Reasonable Expectation of Privacy in Data Held By Home-Sharing Platforms. 8

B. The Ordinance Conscripts Home-Sharing Platforms to Serve as Government Agents and Conduct Searches and Seizures on the City's Behalf. 11

C. The Fourth Amendment Does Not Allow the Government to Manufacture Consent by Compelling Companies to Obtain Such Consent From Their Users 13

III. The Ordinance Violates the Stored Communication Act 15

CONCLUSION 18

TABLE OF AUTHORITIES

Cases

Arizona v. Gant,
556 U.S. 332 (2009) 7

Bond v. United States,
529 U.S. 334 (2000) 10

Byrd v. United States,
138 S. Ct. 1518 (2018) 14

California v. Ciraolo,
476 U.S. 207 (1986) 9

Carpenter v. United States,
138 S. Ct. 2206 (2018) 5, 10

Cassidy v. Chertoff,
471 F.3d 67 (2d Cir. 2006) 11, 12, 13

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 11

Echostar Satellite LLC v. Freetech Inc.,
No. C 07-6124 JW (RS) (N.D. Cal. Sept. 29, 2008) 6

Ferguson v. Charleston,
532 U.S. 67 (2001) 10

Florida v. Jardines,
569 U.S. 1 (2013) 8

Freedman v. Am. Online, Inc.,
303 F. Supp. 2d 121 (D. Conn. 2004) 16

Gonzales v. Google, Inc.,
234 F.R.D. 674, 687 (N.D. Cal. 2006) 6

Katz v. United States,
389 U.S. 347 (1967) 7, 8

Kyllo v. United States,
533 U.S. 27 (2001) 8, 9

Marshall v. Barlow's, Inc.,
436 U.S. 307 (1978) 13

Miller v. United States,
357 U.S. 301 (1958) 9

Minnesota v. Olson,
495 U.S. 91 (1990) 9

Naperville Smart Meter Awareness v. Naperville,
900 F.3d 521 (7th Cir. 2018) 11

Payton v. New York,
445 U.S. 573 (1980) 8, 9

Quon v. Arch Wireless Operating Co.,
529 F.3d 892 (9th Cir. 2008) 15

Rakas v. Illinois,
439 U.S. 128 (1978) 14

Silverman v. United States,
365 U.S. 505 (1961) 8

Skinner v. Railway Labor Executives' Ass'n.,
489 U.S. 602 (1989) 11, 12

Smith v. Maryland,
442 U.S. 735 (1979) 10, 14, 15

Stoner v. California,
376 U.S. 483 (1963) 10, 13

U.S. v. Bennett,
709 F.2d 803 (2d Cir. 1983) 12

U.S. v. Knoll,
16 F.3d 1313 (2d Cir. 1994) 12

United States v. Karo,
468 U.S. 705 (1984) 7, 9

United States v. Miller,
425 U.S. 435 (1976) 10

United States v. Owens,
782 F.2d 146 (10th Cir. 1986) 14

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 15

Statutes

18 U.S.C. § 2510(15) 16

18 U.S.C. § 2707(a) 16

18 U.S.C. § 2711(2) 16

18 U.S.C. §§ 2701–2703 16

Constitutional Provisions

U.S. Const. amend. IV ..... *passim*

Legislative Authorities

H.R. Rep. No. 99-647, to accompany H.R. 4952 (June 19, 1986) 18

New York Civil Liberties Union, Testimony before the New York City Council Committee on Housing and Buildings regarding NYC Council Bill - Int. No. 981-2018 (June 26, 2018) 5

S. Rep. No. 99-541 (1986) 17, 18

Charters

N.Y. Multiple Dwelling Law § 4 6

Administrative Codes

N.Y.C. Admin. Code § 26-2101 ..... 4, 6

N.Y.C. Admin. Code § 26-2102(b) 13

N.Y.C. Admin. Code § 26-2104 13

Other Authorities

Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes As Emails Get Dusty*, 88 B.U. L. Rev. (2008) 17

Albert Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. Ill. U. L. Rev. (1983) 9

Christina Raquel, *Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud*, 55 Santa Clara L. Rev. (2015) 17

Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 Duke L. & Tech. Rev. (2015) 17

Oliva Zaleski, "Airbnb's NYC Bookings Could Be Cut in Half by New Rule," *Bloomberg* (July 24, 2018) 5

Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 Cornell L. Rev. (2010) 8

INTEREST OF AMICUS CURIAE

As an organization focused on users' rights, amicus curiae the Electronic Frontier Foundation (EFF) understands the vital role third-party Internet platforms play in not only connecting individuals with goods and services online, but also in protecting the privacy of those individuals by ensuring that their data is not improperly disclosed. Platforms are firmly embedded in the Internet's current architecture, and Internet users increasingly rely on them to go about their daily lives. To ensure that digital lives are not subject to invasive and undemocratic government searches, EFF believes it is essential that platforms protect their users' privacy. It is likewise essential that platforms' ability to protect their users' privacy is not hamstrung by laws designed to evade existing privacy protections and force platforms to serve the government instead of their users.

EFF is a member-supported, non-profit organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 37,000 members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law to technology. EFF encourages and challenges companies, government, and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society. EFF has filed amicus briefs with this Court in numerous cases applying privacy law to emerging technology. *See*, *e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 134 S. Ct. 2473 (2014); *Maryland v. King*, 133 S. Ct. 1958 (2013); *United States v. Jones*, 565 U.S. 400 (2012); *Ontario v. Quon*, 560 U.S. 746 (2010). EFF also releases an annual "Who Has Your Back" report, which provides objective measurements for analyzing the policies of major technology companies when it comes to handing data to the

government. EFF's "Who Has Your Back" reports focus on specific, measurable criteria that can act as a vital stopgap against unfettered government access to user data.

INTRODUCTION

New York City's recently passed Short-Term Residential Rentals Ordinance compels home-sharing platforms to serve the government instead of their users. The Ordinance conscripts platforms to conduct, on the government's behalf, the very type of invasive searches the Fourth Amendment and Stored Communications Act (SCA) were meant to protect against. The Ordinance requires home-sharing platforms to conduct warrantless searches, on the City's behalf, into how and when City residents are inviting overnight guests into their homes—information that pertains to what these residents do within their own homes. These warrantless searches of what individuals do within their homes are per se unreasonable, and the City cannot escape the warrant requirement by manufacturing an exception to the Fourth Amendment through mandating that platforms obtain their users' consent via Terms of Service provisions. To protect the privacy of the tens of thousands of New Yorkers currently using home-sharing platforms, as well as those considering using these platforms in the future, the City's efforts to circumvent the Fourth Amendment and Stored Communications Act must be rejected.

Providers of Internet platforms have become an increasingly critical conduit in connecting individuals with goods and services in ways that were previously infeasible or even impossible. Home-sharing platforms like Airbnb and HomeAway are examples of such platforms. Like other successful online intermediaries including Craigslist and eBay, these home-sharing platforms are designed to smoothly facilitate transactions between private individuals who would have had a harder time doing business in a pre-Internet age. As a result, like other online intermediaries, home-sharing platforms have become custodians of increasingly voluminous records of their users' transactions—including names, addresses, phone numbers, email addresses, and other personal and financial information, including information regarding

when users were likely at home on a given date and whether they had overnight guests. In the aggregate these records can be extraordinarily revealing of individuals' personal preferences and their activities within their own homes—the heart of Fourth Amendment protection. When used or disclosed improperly, these records implicate serious privacy concerns.

Given the vast amount of sensitive information these platforms hold about what users are doing in their homes, it is essential that users' information is not improperly disclosed to the government without any allegation of wrongdoing, in violation of the Fourth Amendment and the SCA. The Ordinance is the City's attempt to evade these existing legal protections, but the City cannot avoid the requirements of the Fourth Amendment and the SCA by conscripting home-sharing platforms like Airbnb and HomeAway to conduct searches on the City's behalf and by forcing the platforms to obtain their users' blanket consent to these same searches.

This Court should grant Airbnb's and HomeAway's motions for a preliminary injunction.

ARGUMENT

I. The Short-Term Residential Rentals Ordinance Will Sweep in Sensitive and Revealing Data on Tens of Thousands of Innocent Individuals.

The Ordinance forces home-sharing platforms to disclose to the City on an at least monthly basis, and for a potentially unlimited duration, the names, addresses, phone numbers, email addresses, and other personal and financial information of all users who rent out any part of their residences as a "short term rental" via their sites,[1] along with the number of days their homes were rented—information regarding how and when they choose to open their home to overnight guests. *See* N.Y.C. Admin. Code § 26-2101–2105. This information pertains directly

[1] The term "short-term rental" is defined as "a rental for occupancy of fewer than 30 consecutive days of (i) a dwelling unit or part thereof or (ii) housing accommodations within a building." N.Y.C. Admin. Code § 26-2101.

to what individuals are doing inside their homes, and is collected on at least a monthly basis, with potentially unlimited duration.

The Ordinance violates the privacy interests of New York residents who choose to rent their residences on home-sharing platforms by requiring that platforms like Airbnb and HomeAway release this to the City on an ongoing basis, without any allegation of wrongdoing. "Unlike the nosy neighbor who keeps an eye on comings and goings" and who might note that a homeowner has an overnight guest or tenant, home-sharing platforms like Airbnb and HomeAway are "ever alert, and their memory is nearly infallible." *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018). Yet, the Ordinance fails to provide any oversight and privacy protections for information collected about these individuals (and their homes) from the platforms. The Ordinance has no data retention policy, places no prohibitions on sharing data amongst City agencies and officials, and places no limitations on how City agencies or officials may use the data collected. Given the nature of this information, it will be an attractive target of bad actors, so the lack of privacy protections raises security concerns as well.[2]

This Ordinance will impact *all* New Yorkers who rent out space in their homes, not just those who violate the law. The City plans to use the data collected pursuant to the Ordinance to lead a sweeping crackdown on violations of New York's short-term home rental regulations.[3]

---

[2] *See, e.g.*, New York Civil Liberties Union, Testimony before the New York City Council Committee on Housing and Buildings regarding NYC Council Bill - Int. No. 981-2018 (June 26, 2018), available at https://www.nyclu.org/sites/default/files/field_documents/2018.06.26_airbnb_int_981_nyclu_testimony.pdf (testifying that the lack of a data retention policy "creates a likelihood of security breaches").

[3] *See* Oliva Zaleski, "Airbnb's NYC Bookings Could Be Cut in Half by New Rule," *Bloomberg* (July 24, 2018), available at https://www.bloomberg.com/news/articles/2018-07-24/airbnb-s-nyc-bookings-could-be-cut-in-half-by-new-rule.

But the Ordinance Regulation does not just impact those who violate the rules; it also sweeps in data of those who rent out their homes in compliance with New York law.[4]

The threat to privacy interests of "hosts"[5] is palpable. This motion for a preliminary injunction may be the last opportunity for a court to safeguard the interests of these hosts. Once their names are disclosed to the City in February 2019, after the Ordinance goes into effect, there may be little that can be done to protect the individual residents who rent out their residences or rooms in their residences on home-sharing platforms in New York. These residents face grave concerns about their information being released to the City without any allegation of wrongdoing.

Once user information is improperly disclosed to the government, it can be difficult—if not impossible—to effectively remedy such violations. Users of online services know this, and the compelled disclosure of their private information due to a failure of courts to strictly enforce the limitations imposed by the Fourth Amendment and the SCA would understandably undermine user trust and drive users away from even lawful uses of services like Airbnb and HomeAway. *Cf. Gonzales v. Google, Inc.*, 234 F.R.D. 674, 687 (N.D. Cal. 2006) (discussing risk to Google users' privacy from subpoena to Google that sought information about users' search queries); *Echostar Satellite LLC v. Freetech Inc.*, No. C 07-6124 JW (RS), 2008 WL 4460236, at *2 (N.D. Cal. Sept. 29, 2008) (holding that a subpoena requesting a technology

[4] The New York Multiple Dwelling Law, for example, exempts rentals to a "boarder, roomer or lodger," which has been interpreted to mean that, in general, if a guest shares the apartment with a permanent resident who is present for the duration of the rental, it is permissible under the Multiple Dwelling Law. *See* N.Y. Multiple Dwelling Law § 4.

[5] The term "host" is defined in the Ordinance as "a person other than a booking service, including a co-host, who uses a booking service to offer, manage or administer a short-term rental." N.Y.C. Admin. Code § 26-2101.

vendor's customer lists, including individuals whose conduct is not alleged to be illegal, "could lead to the perceived harassment of legitimate users").

Because the Ordinance poses a burden on the privacy interests on hosts, it is crucial that this Court enforce the legal protections afforded to users under the Fourth Amendment and SCA.

II. The Ordinance Violates the Fourth Amendment.

The Fourth Amendment protects against "unreasonable searches and seizures." U.S. Const., amend. IV. "'[S]earches conducted outside the judicial process, without prior approval by judge or magistrate,'" like the searches mandated by the Ordinance, "'are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (citing *Katz v. United States*, 389 U.S. 347, 357 (1967)). The standard is higher when, as here, the search involves the home: "Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances." *United States v. Karo*, 468 U.S. 705, 714–15 (1984). As the Supreme Court has held, "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant." *Id* at 714.

The Ordinance requires home-sharing platforms to conduct warrantless searches, on the City's behalf, into how and when its residents are inviting overnight guests into their home—information that pertains to what these residents do within their owns homes. These warrantless searches do not meet the Fourth Amendment's standard, and the City cannot evade those standards by conscripting platforms to perform searches on its behalf or by mandating platforms to obtain their users' consent via Terms of Service provisions.

A. Users Have a Reasonable Expectation of Privacy in Data Held By Home-Sharing Platforms.

i. The Ordinance Seeks Information About How Residents are Using Their Homes.

"[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *See Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)) (Harlan, J., concurring)). "At the [Fourth Amendment's] very core stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion." *Silverman v. United States*, 365 U.S. 505, 511 (1961). The Constitution explicitly provides, "The right of the people to be secure in their . . . houses . . . shall not be violated." U.S. Const. amend. IV. Thus, while "the Fourth Amendment protects the individual's privacy in a variety of settings[,] . . . [i]n none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms[.]" *Payton v. New York*, 445 U.S. 573, 589 (1980). The Supreme Court has consistently recognized since the Fourth Amendment's ratification that a person's home is sacrosanct—or "the first amongst equals." *Florida v. Jardines,* 569 U.S. 1, 6, 1414–17 (2013) (refusing to permit use of warrantless dog sniff on defendant's porch to "'explore details of the home' . . . that [the officers] would not otherwise have discovered without entering the premises"—was an invasion of the home that violated the Fourth Amendment). The home is the "sacred site" at the heart of the Fourth Amendment. Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 Cornell L. Rev. 905, 913 (2010).

Residents of New York have a reasonable expectation of privacy in the data covered in the Ordinance, information that pertains directly to what individuals are doing inside their

home—precisely, how and when they choose to open their home to overnight guests.[6] The searches mandated by the Ordinance are thus subject to the Fourth Amendment. And the Fourth Amendment is clear: the government may not, without a warrant, intrude on a person's privacy interest in what goes on in their home. *See Kyllo*, 533 U.S. at 33; *Payton*, 445 U.S at 601 (there is an "overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic"); *California v. Ciraolo*, 476 U.S. 207, 213 (1986) ("This area around the home is 'intimately linked to the home, both physically and psychologically,' and is where 'privacy expectations are most heightened.'"); *United States v. Karo*, 468 U.S. 705, 714–15 (1984) ("monitoring of a beeper in a private residence, a location not open to visual surveillance, violates [the] Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence" because the beep could have revealed "a critical fact about the interior of the premises . . . that [the agents] could not have otherwise obtained without a warrant"); *Miller v. United States*, 357 U.S. 301, 307 (1958) ("The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement!").

ii. Users Have a Reasonable Expectation of Privacy in Their Data Regardless of it Being Shared With A Home-Sharing Platform.

Residents who decide to rent out portions of their home on home-sharing platforms do not forfeit their expectation of privacy in the information sought by the Ordinance simply

[6] *Cf. Minnesota v. Olson*, 495 U.S. 91, 96–98 (1990) (overnight guest has reasonable expectation of privacy in home); *see also* Albert Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. Ill. U. L. Rev. 1, 13 (1983) ("[O]ne of the main rights attaching to property is the right to share its shelter, its comfort and its privacy with others.").

because it is shared with platforms like Airbnb or HomeAway. The "third-party doctrine," developed by the Supreme Court in *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), "stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another." *Carpenter*, 138 S. Ct. at 2219. But the Supreme Court's recent landmark ruling in *Carpenter* underscores that the third-party doctrine has never been an on-off switch. "*Smith* and *Miller,* after all, did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate 'expectation of privacy' concerning their contents.'" *Id.* (quoting *Miller* 425 U.S. at 442); *see, e.g., Ferguson v. Charleston*, 532 U.S. 67, 78 (2001) (patient has reasonable expectation of privacy in diagnostic test results held by hospital); *Bond v. United States*, 529 U.S. 334, 338–39 (2000) (passenger retained expectation of privacy in luggage placed in bus overhead bin despite possibility of external inspection by others); *Stoner v. California*, 376 U.S. 483, 489–90 (1963) (hotel guests entitled to constitutional protection even though they provide "implied or express permission" for third parties to access their rooms).

In *Carpenter* itself, the Court refused to apply the third-party doctrine to the government's acquisition of a suspect's cell site location information from his mobile provider because "the seismic shifts in digital technology . . . made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years." 138 S. Ct. at 2219. While the Ordinance may not allow the city to compile an "exhaustive chronicle of location information" as in *Carpenter*, the information the City will collect on a monthly basis for a potentially unlimited duration using the Ordinance is far more revealing than the limited information at issue in *Miller* and *Smith*. *See id*. at 2210. "*Smith* pointed out the limited capabilities of a pen register" used over the course of a mere few days, while *Miller* "noted that

checks were 'not confidential communications but negotiable instruments to be used in commercial transactions.'" *Id.* (quoting *Smith,* 442 U.S. at 725*; Miller*, 425 U. S. at 442); *see also Naperville Smart Meter Awareness v. Naperville*, 900 F.3d 521, 526 (7th Cir. 2018) (finding that residents have a reasonable expectation of privacy in energy-consumption data collected at fifteen-minute intervals via smart meters). Here, although the Ordinance requires home-sharing platforms to turn over information that is implicated in commercial transactions, the information also pertains to what users do in their homes. For example, without access to the platforms' databases, the City would not know exactly how and when individuals choose to open their homes to overnight guests. Residents have a a reasonable of expectation of privacy in this activity going on inside their homes. *See Naperville*, 900 F.3d at 526 (finding that residents have a reasonable expectation of privacy in energy-consumption data collected at fifteen-minute intervals via smart meters).

B. The Ordinance Conscripts Home-Sharing Platforms to Serve as Government Agents and Conduct Searches and Seizures on the City's Behalf.

The City cannot avoid the requirements of the Fourth Amendment by forcing home-sharing platforms to conduct searches on its behalf. It is well settled that a private party becomes an agent of the government when compelled to assist in conducting a search or seizure. *Skinner v. Railway Labor Executives' Ass'n.*, 489 U.S. 602, 614 (1989). According to the Supreme Court, the test is whether, "in light of all the circumstances," the party acted as an "instrument" or agent of the state. *See Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971) (internal quotations omitted). The Second Circuit has held that "a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search for purposes of the Fourth Amendment." *Cassidy v. Chertoff*, 471 F.3d 67 (2d Cir. 2006) (citing

Skinner, 89 U.S. at 614).[7]

In *Skinner,* railroad labor organizers challenged federal regulations that mandated or authorized drug and alcohol testing of railroad employees alleging that the tests conducted by employers after accidents violated the Fourth Amendment. 489 U.S. at 612. The Court held the railroad companies were government agents: "A railroad that complies with the [FRA] regulations does so by compulsion of sovereign authority, and the lawfulness of its acts is controlled by the Fourth Amendment." *Id*. at 614.

Similarly, in *Cassidy*, ferry commuters challenged a Coast Guard-approved security policy that allowed employees of a private ferry operator to conduct random, warrantless searches of passengers. 471 F.3d at 72. The policy was adopted to satisfy requirements imposed by federal regulations. *Id.* The Second Circuit, applying *Skinner*, held that because the searches were instigated by government authority, they constituted governmental searches and were subject to the Fourth Amendment. *Id*. at 74.

Applied here, it is indisputable that the Ordinance seeks to transform home-sharing platforms into government agents to conduct searches of user data on the City's behalf. Indeed, if the Ordinance goes into effect, and if home-sharing platforms begin conducting the mandated searches, they would be doing so for no reason other than compulsion by the Ordinance. The platforms are statutorily obligated not only to perform these searches, but also to hand the results of these searches directly over to the City, and failure to comply opens the platforms up to steep

[7] Other factors relevant to the analysis include whether the government directed the search, knows of and acquiesced to the private party's conduct, and whether the private party intends to aid the government or is conducting the search to achieve its own ends. *See, e.g., U.S. v. Knoll*, 16 F.3d 1313, 1320 (2d Cir. 1994); *U.S. v. Bennett*, 709 F.2d 803, 805 (2d Cir. 1983), revised, 729 F.2d 923 (2d Cir.), cert. denied, 469 U.S. 1075, 105 S.Ct. 572 (1984).

civil penalties. N.Y.C. Admin. Code § 26-2104. As in *Cassidy*, any searches conducted by platforms pursuant to the Ordinance are government searches, instigated by government authority, and are thus subject to the Fourth Amendment. *See* 471 F.3d at 74.[8]

C. The Fourth Amendment Does Not Allow the Government to Manufacture Consent by Compelling Companies to Obtain Such Consent From Their Users.

In another attempt to circumvent the Fourth Amendment, the Ordinance requires that platforms obtain "from each host using [their] booking service to offer, manage or administer a short-term rental, lawful consent to provide the information described in subdivision a to the administering agency." N.Y.C. Admin. Code § 26-2102(b). The Ordinance conveniently provides that "[o]btaining lawful consent may include, but is not limited to, advising or providing notice to a user of the booking service that new or continuing use of such booking service as a host constitutes consent to such disclosure."[9] *Id.* But just as the City cannot avoid the Fourth Amendment by conscripting home-sharing platforms like Airbnb and HomeAway to

[8] The fact that the home-sharing platforms may have legal authority to access the data covered in the Ordinance *for their own purposes* does not change the analysis. *See Stoner v. California*, 376 U.S. 483 (1964) (despite the fact that a hotel owner had legal authority to enter a guest's room, doing so at the police's behest without a warrant violated the Fourth Amendment); *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 315 (1978) (holding that while an employee may enter his work premises and report wrongdoing he sees there, that "furnishes no justification for federal agents to enter a place of business from which the public is restricted and to conduct their own warrantless search").

[9] In the City's Memorandum of Law in Opposition to Plaintiffs' Motions for a Preliminary Injunction, it argues that commonplace terms of service language already appearing on Airbnb's and HomeAway's websites shows that "hosts" have already consented to "the type of disclosure contemplated by [the Ordinance]." *See* ECF No. 27, at 13. Platforms may give notice to their users that they will disclosure information to law enforcement in response to valid legal process, pursuant to valid laws, but this does not give the City free rein to pass unconstitutional laws in order to obtain user data.

conduct its searches, it cannot force platforms to obtain their users' blanket consent to these same searches.

As an initial matter, private contracts such as website terms of service provide a poor vehicle for determining an objective expectation of privacy. These agreements govern the "risk allocation between private parties. . . . But that risk allocation has little to do with whether one would have a reasonable expectation of privacy" absent the contractual term. *Byrd v. United States*, 138 S. Ct. 1518, 1529 (2018). The expectation of privacy analysis is intended to describe "well-recognized Fourth Amendment freedoms," *Smith*, 442 U.S. at 740 n.5, not the interests of private businesses as advanced by form contracts. If terms of service dictated expectations of privacy, private actors could unilaterally set the contours of Fourth Amendment protections; foundational constitutional rights would be determined by which private corporations an individual chooses to do business with. Worse still, the government could avoid its constitutional duties by conscripting private actors to mandate its chosen contractual terms.

Fortunately, that is not the law. Just as the Supreme Court has cautioned "that arcane distinctions developed in property and tort law . . . ought not to control" the analysis of who has a "legally sufficient interest in a place" for Fourth Amendment purposes, *Rakas v. Illinois*, 439 U.S. 128, 142-43 (1978), courts have declined to find private contracts dispositive of individuals' expectations of privacy. In *Smith*, the Supreme Court noted, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." *Smith*, 442 U.S. at 745. And just this year in *Byrd,* the Court declined to find that a driver forfeited his right to privacy by violating a car rental agreement. 138 S. Ct. at 1529; *see also, e.g., United States v. Owens*, 782 F.2d 146, 150 (10th Cir. 1986) (finding that motel's private terms did not void

guest's expectation of privacy because "[a]ll motel guests cannot be expected to be familiar with the detailed internal policies and bookkeeping procedures of the inns where they lodge"); *Quon v. Arch Wireless Operating Co.,* 529 F.3d 892 (9th Cir. 2008) (holding that users have reasonable expectation of privacy in text messages, despite advance warning that the messages could be read), *rev'd on other grounds,* 560 U.S. 746 (2010). For that reason, provisions in the platforms' current terms of services that discuss sharing user information with law enforcement do not by themselves vitiate users' expectations of privacy. *See United States v. Warshak*, 631 F.3d 266, 286–87 (6th Cir. 2010) (term of service granting the "*right* of access" or "the mere ability . . . to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy") (emphasis in original).

The consent provision in the Ordinance is doubly problematic because it is mandated by the government rather than freely adopted by the home-sharing platforms themselves. It is axiomatic that the government cannot eliminate Fourth Amendment rights by fiat, such as by "announc[ing] on nationwide television that all homes henceforth would be subject to warrantless entry." *Smith*, 442 U.S. at 741 n.5. The consent required by the Ordinance is plainly an attempt to manufacture an exception to the Fourth Amendment, and it should be rejected.

III. The Ordinance Violates the Stored Communication Act.

As outlined in Airbnb's memorandum of law in support of its motion for preliminary injunction, the SCA provides that the government may not obtain subscriber information from entities like Airbnb, that qualify as electronic communication services and/or remote computing

services,[10] without either presenting a grand jury subpoena, trial subpoena, or administrative subpoena authorized by federal or state law, or directly obtaining the users' consent. ECF No. 14-1, 24–25. Compliance with the Ordinance, which does not provide for any legal process of any kind, would violate the SCA's protections for user data. The City cannot evade the SCA's protections by forcing home-sharing platforms to obtain their users' blanket consent for the same reasons it cannot use this tactic to evade the Fourth Amendment's protections. *See also Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121, 129 (D. Conn. 2004) ("[T]he statute clearly instructs that the burden is on the governmental entity to obtain consent[.]").

Congress passed the Electronic Communications Privacy Act (ECPA) in 1986, in response to concerns that electronic communications were inadequately protected from unauthorized access. Title II of ECPA, the SCA, criminalizes unauthorized access to users' stored communications, prohibits Internet service providers from voluntarily sharing those communications, and restricts the government's ability to request user data from those providers. 18 U.S.C. §§ 2701–2703. The SCA also provides a private civil remedy for violations of its protections. *See* 18 U.S.C. § 2707(a).

The legislative history reflects that in passing ECPA and the SCA, Congress sought to codify Fourth Amendment-like protection for stored electronic communications and to provide privacy protection for data relating to these important new methods of communication. As a 1986 Senate report accompanying the bill noted, "[T]he law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment. Privacy cannot be left to depend

[10] An electronic communication service ("ECS") allows for the sending or receiving of electronic communications, 18 U.S.C. § 2510(15), while a remote computing service ("RCS") provides storage or processing services. 18 U.S.C. § 2711(2).

solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens." S. Rep. No. 99-541: Electronic Communications Privacy Act of 1986, to accompany S. 2575, at 5 (Oct. 17, 1986), reprinted at 1986 U.S.C.C.A.N. 3555, 3559; *see also* Christina Raquel, *Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud*, 55 Santa Clara L. Rev. 467, 479 (2015) (citing Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes As Emails Get Dusty*, 88 B.U. L. Rev. 1043, 1054 (2008) ("The Electronic Communications Privacy Act of 1986 ('ECPA') represents a Congressional endeavor to prevent the Fourth Amendment's third party doctrine from compromising the privacy interests of electronic communications stored by third parties.").

Congress recognized in passing ECPA and the SCA that in order to promote technological advancement, it was necessary to ensure that users could be confident in the privacy of their stored electronic communications and data regarding their electronic communications. Congress thus sought to provide a baseline of protection to "encourage the commercial use of 'innovative communications systems,' and discourage unauthorized users from obtaining access to communications to which they are not a party[.]" Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 Duke L. & Tech. Rev. 36, 41 (2015) (citing S. Rep. No. 99-541, at 5 (1986)). As the committee reports accompanying ECPA reflect, Congress was well aware of the need to protect against unauthorized access of user data, both so that providers would not be deterred from offering new services and that potential customers would not be deterred from using them. The 1986 House Judiciary Committee Report, for example, pointed to the danger of the deficiencies of existing legal protections: "In the absence of market discipline, there is no presumption that the government will strike an appropriate balance between disclosure and

confidentiality. And the enormous power of the government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm." H.R. Rep. No. 99-647: Electronic Communications Privacy Act of 1986, to accompany H.R. 4952, at 19 (June 19, 1986) (quoting Posner, *Privacy in the Supreme Court*, 1979 Sup. Ct. Rev. 173, 176 (1979)) (alterations in original). The committee worried that such "legal uncertainty" may "unnecessarily discourage potential customers" from relying on new communications systems and stated that "if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right." *Id*. Meanwhile, the Senate Judiciary Report noted that the lack of federal privacy and security standards for communications transmitted via "new forms of telecommunications and computer technology" may not only discourage potential customers from using innovative communications systems, but also discourage American businesses from developing new innovative forms of telecommunications and computer technology. S. Rep. No. 99-541, at 5.

As this legislative history makes clear, Congress intended the SCA to ensure that users of technology platforms could have confidence that Internet service providers would respect the privacy of their electronic records and would not disclose their records to law enforcement without appropriate legal process. The Ordinance undermines this confidence, by compelling home-sharing platforms to serve the government instead of their users. The Ordinance is in direct conflict with Congress's intent. To protect users, this Court should enforce the privacy protections set out by Congress in the SCA.

CONCLUSION

This Court should grant Airbnb's and HomeAway's motions for a preliminary injunction.

San Francisco, California
Dated: October 1, 2018

Respectfully submitted,

/s/ Mitchell L. Stoltz

Mitchell L. Stoltz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: 415-436-9333
Fax: 415-436-9993
Email: mitch@eff.org

CERTIFICATE OF COMPLIANCE

I, Mitchell L. Stoltz, counsel for amicus curiae Electronic Frontier Foundation, hereby certify that according to the word count feature of the word processing program used to prepare this brief, the brief contains 5,389 words and 18 pages (exclusive of the cover page, certificate of service, certificate of compliance, table of contents, and table of authorities), and complies with Local Civil Rule 11.1 of the Southern District of New York, as well as with Individual Practice Rule 3(C) of Judge Paul A. Engelmayer.

/s/ Mitchell L. Stoltz

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the accompanying brief for amicus curiae Electronic Frontier Foundation by using the CM/ECF system on October 1, 2018.

I certify that all participants in the case are registered CM/ECF users and that serviced will be accomplished by the CM/ECF system.

Dated: October 1, 2018

/s/ Mitchell L. Stoltz